Claims

1. A circuit arrangement for securing communication between network subscribers belonging to a peer-to-peer network, comprising
a network module for communication with the further network subscribers and external communications devices (servers) that do not belong to the peer-to-peer network,
a crypto module for handling cryptographic functions, a first memory module (SM1) comprising memory sub-modules in which association features (PA, ZA, ZCA) relating to a first network subscriber are stored, wherein a second memory module (SM2) is provided, with the second memory module (SM2) comprising memory sub-modules (SMX, SMY, ...) for buffering certificates (ZX, ZY, ...) of further network subscribers (peer X, peer Y, ...) and it being possible for the certificates of these further network subscribers to be requested by all other network subscribers (peer N, peer M, ...) in each case.

2. The circuit arrangement as claimed in claim 1, wherein the external communications device is characterized in such a way that digital certificates can be produced and stored in the second memory module (SM2).

3. The circuit arrangement as claimed in any one of the preceding claims, wherein the arrangement is disposed in the first network subscriber.

4. A method for securing communication between network subscribers belonging to a peer-to-peer network, comprising
a network module for communication with the further network subscribers and external communications devices (servers) that do not belong to the peer-to-peer network,

a crypto module for handling cryptographic functions, a first memory module (SM1) comprising memory sub-modules in which association features (PA, ZA, ZCA) relating to a first network subscriber are stored, wherein a second memory module (SM2) is divided into memory sub-modules (SMX, SMY, ...) for buffering certificates (ZX, ZY, ...) of further network subscribers (peer X, peer Y, ...) and the certificates of these further network subscribers may be requested by all other network subscribers (peer N, peer M, ...) in each case.

5. The method as claimed in claim 4, wherein the digital certificates are created in the external communications device and can be stored in the second memory module (SM2).